CHAPTER 24.

READING GENERATIVE AI TERMS OF SERVICE IS A WASTE OF TIME

✨ *READING GENERATIVE AI TERMS OF SERVICE SUPPORTS A BROADER UNDERSTANDING OF TECHNOLOGY'S IMPACT*

Morgan C. Banville
Fairfield University

Charles Woods
East Texas A&M University

It is a "bad idea" for instructors to *not* read Terms of Service (ToS) documents with students before using generative artificial intelligence (GenAI) in the classroom because data students generate is used to train GenAI without informed consent, allowing Big Technology (BigTech) and Educational Technology (EdTech) companies to profit from instructor—and student—data and labor. It is a better idea to use ToS documents for GenAI to teach critical AI literacies through frameworks such as Interlocking Surveillance (IS) and Digital Rhetorical Privacy (DRP).

Our chapter is focused on instructors and how they incorporate different digital technologies in the classroom. We believe GenAI is incorporated into the classroom without necessary critical examination of the consequences by instructors and their students. Instructors should read the ToS with students to address such consequences together. As Whitney Lew James (2026) explains, "because GenAI systems produce better results with more user information, we are encouraged to share personal information with these companies." We resonate with her claim, and in our role as instructors, we connect the assignments and activities to the programmatic or course-specific learning outcomes with career preparedness in mind. But we believe instructors also have a responsibility to engage in discussions about data privacy with their students if they are going to integrate GenAI into the classroom.

DOI: https://doi.org/1010.37514/PER-B.2026.2777.2.24

ToS are written to protect a company legally, which we think necessitates complex interrogations of ToS documents governing GenAI (Beck, 2016). Furthermore, Timothy R. Amidon et al. (2019) detail the ethical and legal tensions for intellectual property (IP). Scholars like Morgan C. Banville (2020), Charles Woods and Gavin P. Johnson (2024), and Rachel Jordan (2024) theorize the implications that ToS documents have on medical surveillance, digital privacy, and queer bodies. Understanding the implications of data collected via AI is complex, therefore the aforementioned scholars focus on specific cultures and communities: How does medical surveillance impact bodily autonomy? What does subverting surveillance for sex worker networks look like? Focusing on data privacy in specific communities makes the enormity of digital data collection recognizable, and we believe our better idea of reading the ToS with students before using GenAI is an effective way to make these issues tangible.

TWO METHODOLOGICAL FRAMEWORKS FOR READING TERMS OF SERVICE

Data students generate is used to train GenAI, contributing to a culture of surveillance capitalism. Zuboff (2019) describes the hallmark of this concept as companies profiting off individual user data via targeted advertising. As a result, and understandably, instructors hold a variety of opinions and arguments regarding AI (and more specifically, GenAI). For example, some instructors necessitate using AI for career readiness whereas others actively resist using AI because of social, environmental, and technological factors.

Instructors must untangle the complex relationship among students, universities, and EdTech companies to understand issues of IP, copyright, and data commodification. In fact, Marit MacArthur details AI's "vampiric reliance on 'training data'—a euphemism, in this context, for human generated writing" in the next chapter. Here, we offer a more generative idea for studying AI—two frameworks that instructors can use to understand these implications: Banville's (2023) Interlocking Surveillance (IS) and Woods' (2021) Digital Rhetorical Privacy (DRP). IS and DRP offer renewed methodological approaches to understanding privacy and surveillance in relation to informed consent. We illustrate the ways in which each framework is effective for investigating how data collected from our students is used to train GenAI. Our goals are to amplify learning about data privacy issues and surveillance when using GenAI, for example, and to offer clear methodological approaches for doing so. IS and DRP are effective frameworks for these complex investigations.

Banville (2023) argues that IS can inform decision-making processes into sites of resistance and advocacy, extending scholarship regarding surveillance

technologies (Lyon, 2007) through an intersectional (Crenshaw, 1989) approach to data collection, coding, and analysis. IS recognizes and confronts power imbalances maintained over audiences, who are "often not informed of such collection" (Lindgren et al., 2023, p. 111). The goal of interlocking surveillance is to call attention to the ways technical communicators and instructors may make suggestions and intervene in processes to advocate (for users), create awareness (through accessible language and materials), and communicate transparency (about data collection and practices) (Banville, 2023). The following IS heuristic assesses "sites" of surveillance (Lyon, 2007) by accounting for the collection of visible and invisible data derived from those being observed (Banville, 2023):

- What are the intended purposes of the technology?
- How does the corporation justify its standard usage?
- How does it categorize people and into what categories (and for what purpose)?
- How does the corporation justify its technological usage?
- How are people informed about the capabilities, data collection, and more?
- Is the technology poised for efficiency purposes, or implemented during a time of "urgency"? (p. 145)

Some students may say "I don't care about ChatGPT taking my information/data" and "I don't mind training the AI." Other than accuracy, reliability, and labor exploitation (Perrigo, 2023), one concern related to implementing GenAI such as the infamous ChatGPT in the classroom space, for example, is IP. Any time that instructors and students alike use a tool that needs an account, the company now has an identifier in which they can surveil user usage of the site and match that to specific identities. Also, users usually need to provide personally identifiable information such as an "email/phone number/Google account" to create an OpenAI account (2024). As Tim Laquintano et al. (2023) note, large language models include massive datasets that are drawn on to make predictions. Importantly, they also note that OpenAI has been coy about sharing data sources for "safety reasons and to retain a competitive edge" (Laquintano et al., 2023). Further, many of the concerns with IP overlap with other concerns such as labor issues: using GenAI is providing free labor (surveillance capitalism) to OpenAI, for example, in their product development. They are clear about this in their terms and in their FAQ page[1] (OpenAI, 2024). The generators learn

1 According to OpenAI (2024), "We may use content submitted to ChatGPT, DALL·E, and our other services for individuals to improve model performance. For example, depending on a user's settings, we may use the user's prompts, the model's responses, and other content such as images and files to improve model performance."

and are trained by not only the information scraped from the web, but also the information inserted into the model.

Informed consent is at the crux of both IS and DRP. As a theory, DRP helps instructors understand privacy erosion amid unethical surveillance. It considers data privacy as rhetorical, and privacy as a "state of being when a user is confident their digital data is free from unauthorized observances by nefarious computer technologies and other users" (Woods, 2021, p. 5). Additionally, defining "nefarious" in this context means looking at the data that is collected and how it is used. Thus, DRP accounts for the cultural aspects of privacy to underscore how surveillance supports oppressive social, political, and economic infrastructures. DRP integrates inherently intertwined analytic elements to construct a framework for analyzing ToS documents, including:

- Temporality
- Transparency
- Language
- Data Usage
- Digital Surveillance
- Meaningful Access
- Design

To illustrate this further, we have an example from the IS and DRP frameworks: One question in the IS heuristic asks, **how are people informed about the capabilities, data collection, and more?** From OpenAI's ToS, we found that the only way users are informed about capabilities is if they read the ToS. In them, there are steps that users can take to "opt out" of data collection; however, users must read the terms to be informed about this option.[2]

The DRP framework considers transparency by asking, **what relationships does the publisher of the policy maintain with third-parties?** The Google Gemini Apps Privacy Notice (Google, 2025) explains user data is shared across Google services and with third-parties. This could include government stakeholders and other BigTech companies through contracts and collaborations. Interestingly, data from Gemini is processed by human reviewers, not only machines, which creates a different hurdle in understanding transparency.

Our frameworks give instructors options for how they might approach analysis and careful integration of AI that keeps decision-making and informed consent at the forefront. Daniel Fitzpatrick et al. (2023) write, "outsource your

2 "You can opt out of training through our privacy portal by clicking on 'do not train on my content,' or to turn off training for your ChatGPT conversations, follow the instructions in our Data Controls FAQ. Once you opt out, new conversations will not be used to train our models" (OpenAI, 2024).

doing, not your thinking" (p. 33), suggesting that instructors should carefully consider when they should allow students to use GenAI in their learning. For example, instructors can use the frameworks to unpack *what* AI can and should be used for within the classroom. Sure, GenAI in particular can assist with learning objectives, activities, developing assessments, and more, but should the GenAI be fed student work to "provide feedback?" Likely not. Though some instructors have posited that AI can be useful for providing effective feedback, such articles do not describe how instructors are protecting students from threats to copyright and IP. As Ethan Mollick and Lilach Mollick (2023) write, despite their support of instant feedback, students should examine biases and not take the work of AI "too seriously." How, as instructors, do we teach students to consider risks and benefits, as well as "not take the work of the AI too seriously"? Students *do* take feedback seriously and are not likely considering biases or misinformation. It would be a bad idea to incorporate AI as a means of giving feedback to students, especially without reading the ToS first.

CONCLUSION

Instructors can prepare students to effectively use GenAI by critically evaluating the new writing technologies that students adopt. AI has a range of surveillant impacts on legal compliance, security concerns, and accuracy. Reading the ToS with students amplifies these issues for them, including those related to IP. We therefore offer two last considerations to protect IP:

- Have students register with "burner accounts," which can be defined as temporary or anonymous profiles that are not linked to personal information such as real names or addresses (additionally, burner accounts are always a good idea to use for social media experiments in the classroom). For example, Apple can create a substitute email with the "Hide My Email" feature.
- Also, this changes constantly but there are some applications such as DeepAI AI Image Generator and Google Gemini that will allow students to utilize GenAI "anonymously" and without signing in. It is important that instructors provide alternate assignments if a student objects to using a commercial application.

Whether or not we decide to implement GenAI in the classroom, instructors should still have conversations with students about topics such as intellectual property, data privacy, and surveillance. They should read the ToS documents with students. Doing so adheres to Noël Ingram's argument that we should not AI proof our classrooms and could propel students into a scaffolded unit wherein

they are included in GenAI policymaking for the class, as Annika Hauser-Brydon et al. argue later in this collection. Ultimately, IS and DRP offer frameworks to perform these investigations effectively.

REFERENCES

Amidon, T. R., Hutchinson, L., Herrington, T., & Reyman, J. (2019). Copyright, content, and control: Student authorship across educational platforms. *Kairos, 24*(1). http://kairos.technorhetoric.net/24.1/topoi/amidon-et-al/index.html

Banville, M. C. (2020, October 03–04). Resisting surveillance: Responding to wearable device privacy policies. *SIGDOC '20: Proceedings of the 38th ACM International Conference on Design of Communication, 29*, 1-8 https://doi.org/10.1145/3380851.3416764

Banville, M. C. (2023). *Am I who I say I am? The illusion of choice: Biometric identification in healthcare* (Publication No. 30603350). [Doctoral dissertation, East Carolina University]. ProQuest Dissertations & Theses Global

Beck, E. (2016). Who is tracking you? A rhetorical framework for evaluating surveillance and privacy practices. In S. Apostel & M. Folk (Eds.). *Establishing and evaluating digital ethos and online credibility*, (pp. 66-84). IGI Global.

Crenshaw, K. W. (1989). Demarginalizing the intersection of race and sex: A black feminist critique of antidiscrimination doctrine, feminist theory and antiracist politics. U*niversity of Chicago Legal Forum, 1*, 139-167.

Fitzpatrick, D., Fox, A., & Weinstein, B. (2023). *The AI classroom: The ultimate guide to artificial intelligence in education*. TeacherGoals Publishing, LLC.

Google. (2025, September 2) Gemini apps privacy hub. https://support.google.com/gemini/answer/13594961?hl=en

Hauser-Brydon, A., Smith, M., Walker, J., Byle, S., Theders, N., Thornton, J., Fedewa, K., & DeVoss, D. N. (2026). Exclude students from institutional conversations and policy making around AI: Students should be included in institutional AI policy conversations. In C. Basgier, A. Mills, M. Olejnik, M. Rodak, & S. Sharma (Eds.), *Bad ideas about AI and writing: Generative practices for teaching, learning, and communication*. The WAC Clearinghouse; University Press of Colorado. https://doi.org/10.37514/PER-B.2026.2777.2.47

Ingram, N. (2026). We should suspect our students are using AI: Instead of mistrusting our students, we should embrace a pedagogy of trust and joy. In C. Basgier, A. Mills, M. Olejnik, M. Rodak, & S. Sharma (Eds.), *Bad ideas about AI and writing: Generative practices for teaching, learning, and communication*. The WAC Clearinghouse; University Press of Colorado. https://doi.org/10.37514/PER-B.2026.2777.2.40

James, W. L. (2026). Gen AI can be accessed for free: AI poses significant hidden costs to individuals, society, and the planet. In C. Basgier, A. Mills, M. Olejnek, M. Rodak and S. Sharma (Eds.). *Bad ideas about AI and writing: Generative practices for teaching, learning, and communication*. WAC Clearinghouse; University Press of Colorado. https://doi.org/10.37514/PER-B.2026.2.22

Jordan, R. (2024). Studying surveillance through hybrid concealment practices: A queer analysis of digital sex work safety guides. *Peitho: Journal of the Coalition of Feminist Scholars in the History of Rhetoric, 21*(1), 211-225.

Laquintano, T., Schnitzler, C., & Vee, A. (2023). An introduction to teaching with text generation technologies. In A. Vee, T. Laquintano, & C. Schnitzler (Eds.), *TextGenEd: Teaching with text generation technologies*. The WAC Clearinghouse. https://doi.org/10.37514/TWR-J.2023.1.1.02

Lindgren, C., Banville, M., & Kalodner-Martin, E. (2023). Show your work! Three qualitative methodologies to revise and reimagine quantitative work as communication design. *SIGDOC '23: Proceedings of the 41st ACM International Conference on Design of Communication*, 110–111. https://doi.org/10.1145/3615335.3623019

Lyon, D. (2007). *Surveillance studies*. Polity Press.

Mollick, E., & Mollick, L. (2023, September 25). Part 1: AI as feedback generator. *Harvard Business Publishing Education*. https://hbsp.harvard.edu/inspiring-minds/ai-as-feedback-generator

OpenAI. (2024, September). *Data usage for consumer services FAQ*. https://help.openai.com/en/articles/7039943-data-usage-for-consumer-services-faq

Perrigo, B. (2023, January 18). Exclusive: OpenAI used Kenyan workers on less than $2 per hour to make ChatGPT less toxic. *Time*. https://time.com/6247678/openai-chatgpt-kenya-workers/

Woods, C. (2021). *Interrogating digital rhetorical privacy on direct-to-consumer genetics websites* (Dissertation No. 28645031) [Doctoral dissertation, Illinois State University]. ProQuest Dissertations & Theses Global. https://login.proxy.tamuc.edu/login?url=https://www.proquest.com/pqdtglobal1/dissertations-theses/interrogating-digital-rhetorical-privacy-on/docview/2585863383/sem-2?accountid=7083

Woods, C., & Johnson, G. P. (2024). (Re)Designing privacy literacies in the age of generative AI. *Communication Design Quarterly, 12(2), 86-97*. https://doi.org/10.1145/3655727.3655736

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Profile Books.